CSE302 – Theory of Computation

2.1 Mathematical Terms and Theory

Topics to be covered

- Set
- Logic
- Function
- Relation
- Languages

Set

Set

- A set is a collection of objects.
- The objects in a set are called elements of the set.
- Examples:

1. A = {11, 12, 21, 22}
2. B = {11, 12, 21, 11, 12, 22}

Roster Notation

3. C = {x | x is odd integer greater than 1}
4. D = {x | x Є B and x ≤ 11}

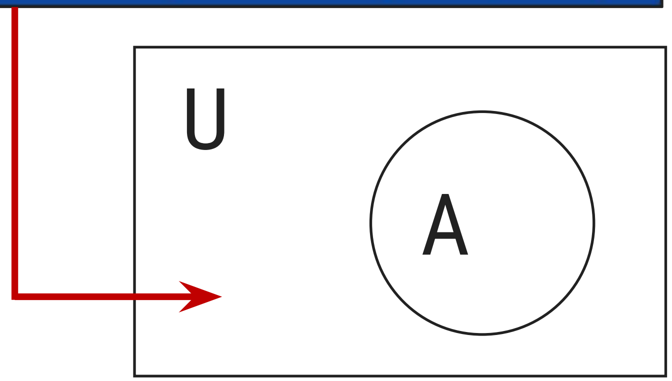
Set-builder Notation

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The complement of a set A is the set A' of everything that is not an element of A from Universal Set U.

$$A' = \{x \in U \mid x \notin A\}$$



- Example:

  U = {1,2,3,4,5}

  A = {1,2}

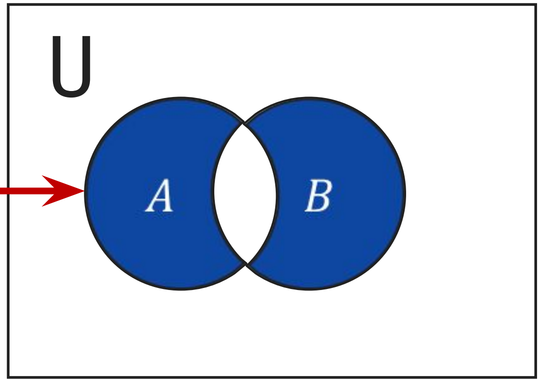
  A' = {3,4,5}

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The Union $(A \cup B)$ is a collection of all distinct elements from both the set A and B.

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$



- Example:

  A = {1, 3, 5, 7, 9}

  B = {1, 2, 3, 4, 5}

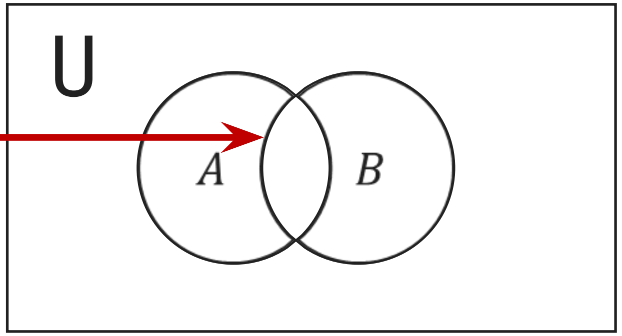
  A U B = {1, 2, 3, 4, 5, 7, 9}

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The intersection $A \cap B$ of two sets A and B is the set that contains all elements of A that also belong to B, but no other elements.

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$



- Example:

  A = {1, 3, 5, 7, 9}

  B = {1, 2, 3, 4, 5}

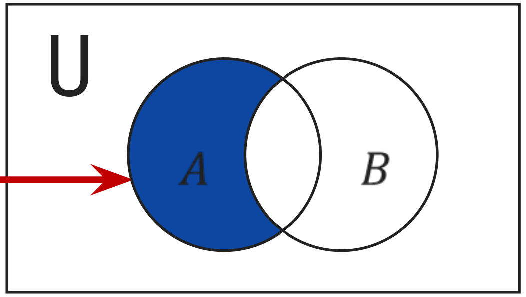
  $A \cap B$ = {1, 3, 5}

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The set difference A - B of two sets A and B is the set of everything in A but not in B.

$$\begin{aligned} A - B &= \{x \mid x \in A \text{ and } x \notin B\} \\ &= \{x \mid x \in A\} \cap \{x \mid x \notin B\} \\ &= A \cap B' \end{aligned}$$



- Example:

  A = {1, 3, 5, 7, 9}

  B = {1, 2, 3, 4, 5}

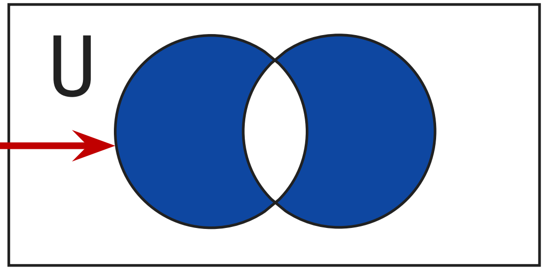
  A - B = {7, 9}

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The symmetric difference $A \ominus B$ of two sets A and B is the set of everything in A but not in B or the set of everything in B but not in A.

$$A \ominus B = (A - B) \cup (B - A)$$



- Example:

  A = {1, 3, 5, 7, 9}

  B = {1, 2, 3, 4, 5}

  $A \ominus B$ = {7, 9, 2, 4}

Operations on Sets

- Operations on the sets are:
  1. Complement
  2. Union
  3. Intersection
  4. Set Difference
  5. Symmetric Difference
  6. Cartesian product

- The Cartesian product A x B of two sets A and B is the set of all ordered pairs (a, b) where a ∈ A and b ∈ B.

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

- Example:

  A = {1, 3, 5}

  B = {2, 4}

  A x B = {(1,2), (1,4), (3,2), (3,4), (5,2), (5,4)}

Set of identities

- Commutative laws

$$A \cap B = B \cap A$$
$$A \cup B = B \cup A$$

- Associative laws

$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \cup (B \cup C) = (A \cup B) \cup C$$

- Distributive laws

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Set of identities

- Idempotent laws

$$A \cup A = A$$
$$A \cap A = A$$

- Absorptive laws

$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

- De Morgan laws

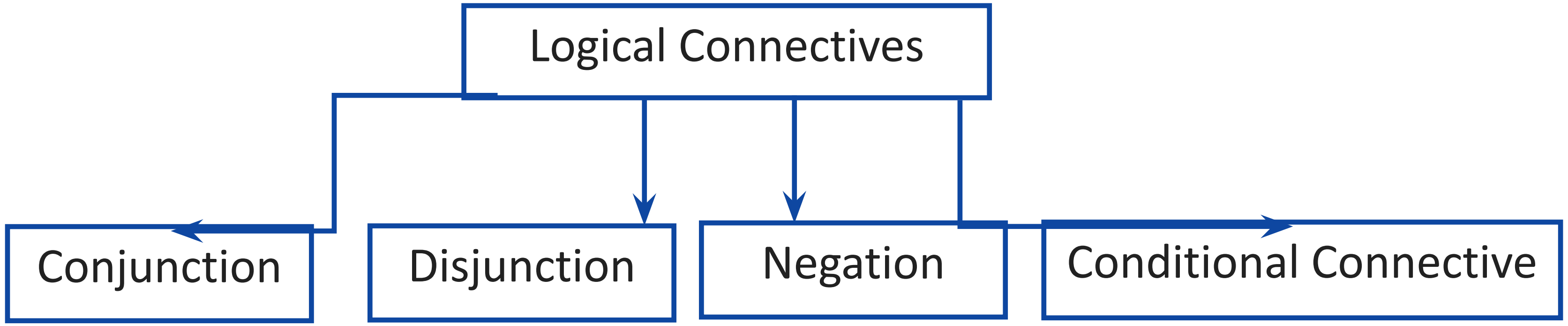
$$(A \cup B)' = A' \cap B'$$
$$(A \cap B)' = A' \cup B'$$

Logic

Propositions

- Declarative statement that is sufficiently objective, meaningful and precise to have a truth value (true or false) is known as proposition.
- Examples:
  1. p : Fourteen is an even integer.
  2. r : 0 = 0
  3. q : Mumbai is the capital city of India.
  4. s : $a^2+b^2=4$

Logical Connectives

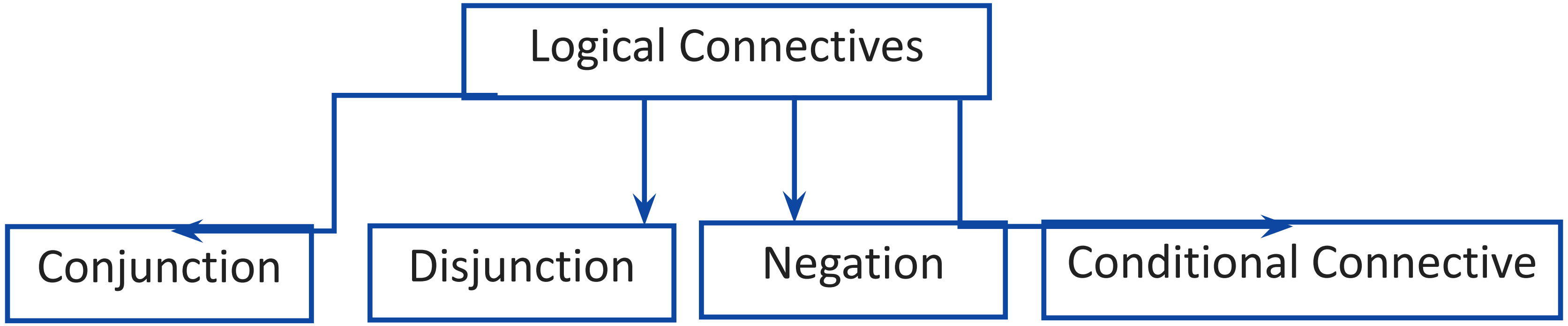


- The logical connective Conjunction (And) is true only when both of the propositions are t

p	q	r = p ^ q
True	True	True
True	False	False
False	True	False
False	False	False

- Example:
-
  - p : It is raining
  - q : It is warm
  - r : It is raining **AND** it is warm

Logical Connectives



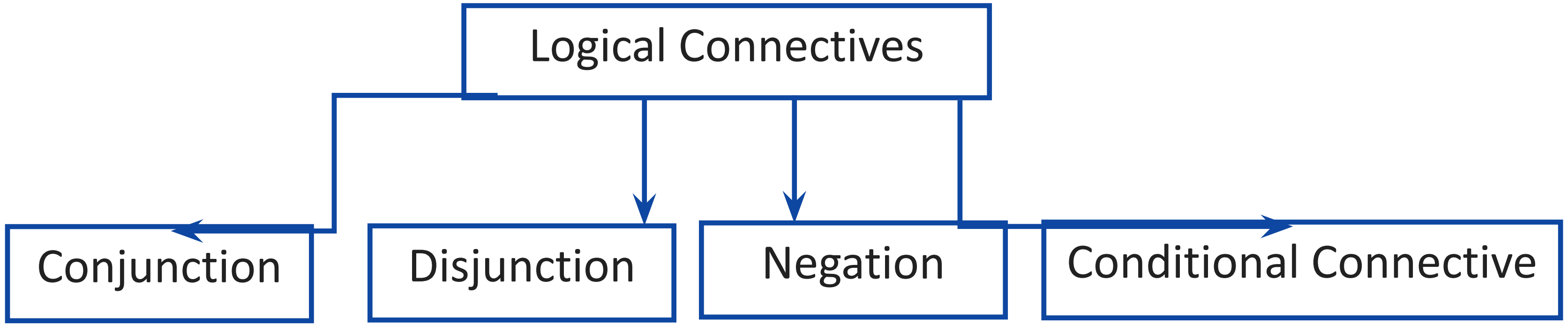
- The logical disjunction, or logical OR, is true if one or both of the propositions are true.

p	q	$r = p \vee q$
True	True	True
True	False	True
False	True	True
False	False	False

Truth table

- Example:
  - p : $2 + 2 = 5$
  - q : $1 < 2$
  - r : $2 + 2 = 5$ **OR** $1 < 2$

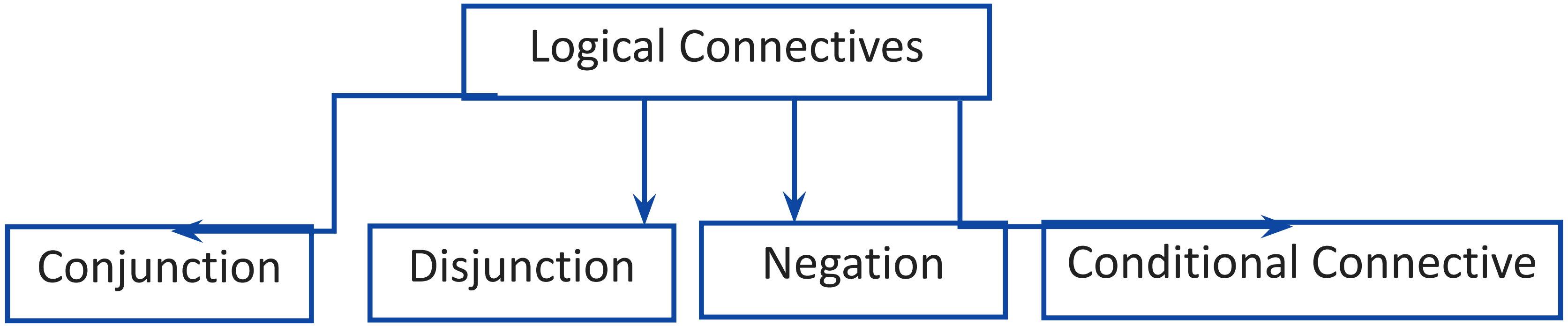
Logical Connectives



- ¬p, the negation of a proposition p, is also a proposition.
- Example:
- Truth table
    - p : John studies.
    - ¬p : John does **NOT** study.

P	¬P
True	False
False	True

Logical Connectives



- The proposition p → q is commonly read as “if p then q”.
- Example: P→ I will win the lottery. Q→ I will buy car for you.

I win the lottery	I will buy car for you	Promise kept/ broken
Yes	Yes	Kept
Yes	No	**Broken**
No	Yes	Not broken
No	No	Not broken

p	q	p□q
True	True	True
True	False	False
False	True	True
False	False	True

Functions

Functions

- Domain: What can go into the function is called domain.
- Codomain: What may possibly come out from a function is codomain.
- Range: What actually come out from a function is range. The range of function is subset of codomain
- Example:

$$f: N \to N, f(x) = 2x + 1$$

f(1)=2(1)+1= 3

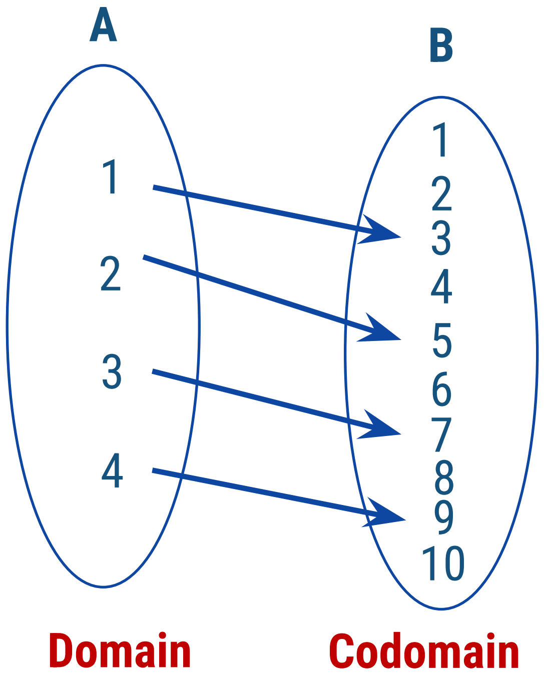
f(2)=2(2)+1= 5

f(3)=2(3)+1= 7

f(4)=2(4)+1= 9

- The range of function $f(x) = \{3, 5, 7, 9\}$

Range



Onto Function

- If the range of function and codomain of function are equal or every element of the codomain is actually one of the values of the function, then function is said to be onto or surjective or surjection.
- Example: $f : A \rightarrow B, f(x) = x^2$ where,

  A = {-2,-1,1,2,3,4} and B = {1,4,9,16}

  f(-2) = 4

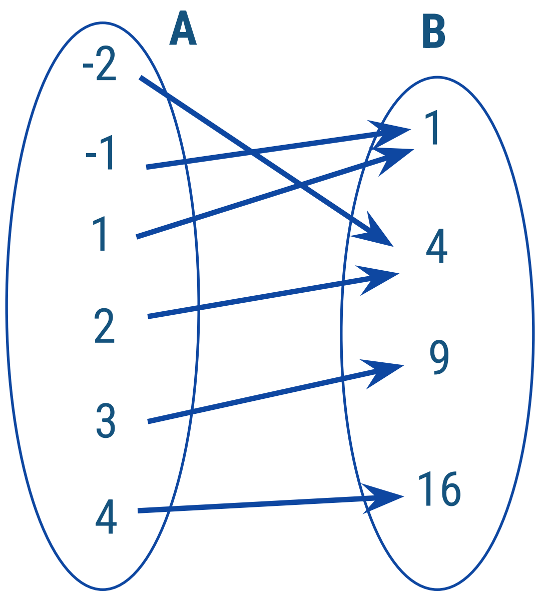
  f(-1) = 1

  f(1) = 1

  f(2) = 4

  f(3) = 9

  f(4) = 16



- The range of function f(A) = {1, 4, 9, 16} = B

One-to-One Function

- A function for which every element of the range of the function corresponds to exactly one element of the domain is known as One-to-One or injective or injection.
- Example: $f : A \to B, f(x) = x^2$ where,

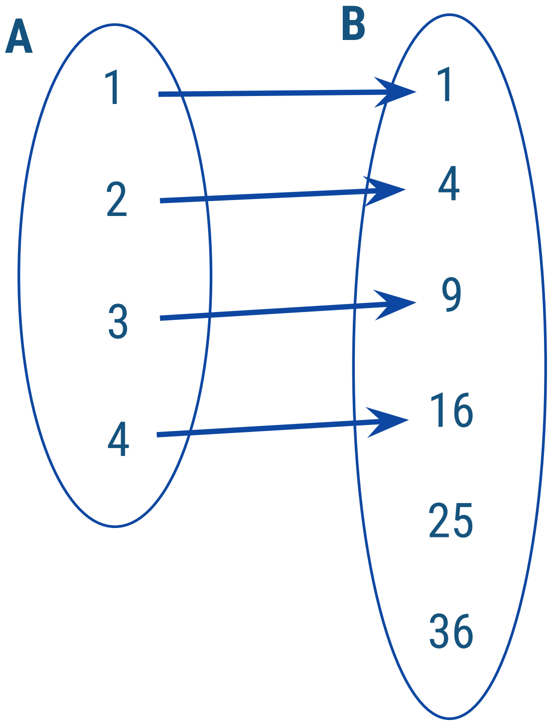
  A = {1,2,3,4} and B = {1,4,9,16,25,36}

f(1) = 1

f(2) = 4

f(3) = 9

f(4) = 16



Bijection Function

- If function is both one-to-one and onto then function is called Bijection function.
- Example: $f : A \to B, f(x) = x^2$ where,

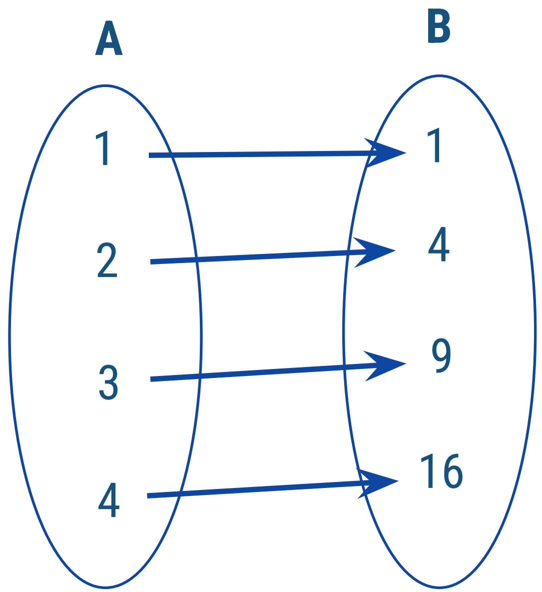
  $A = \{1,2,3,4\}$ and $B = \{1,4,9,16\}$

  f(1) = 1

  f(2) = 4

  f(3) = 9

  f(4) = 16



Relations

Relations

- A relation on a set A is defined as subset of $A \times A$.
- The relation R is denoted as aRb where $a, b \in A$ and pair $(a, b) \in R$.
- Example:

$$N = \{1,2,3\}$$
$$N \times N = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}$$

- The '=' relation on $N \times N$ is : $\{(1,1), (2,2), (3,3)\}$

  where

  1 = 1

  2 = 2

  3 = 3

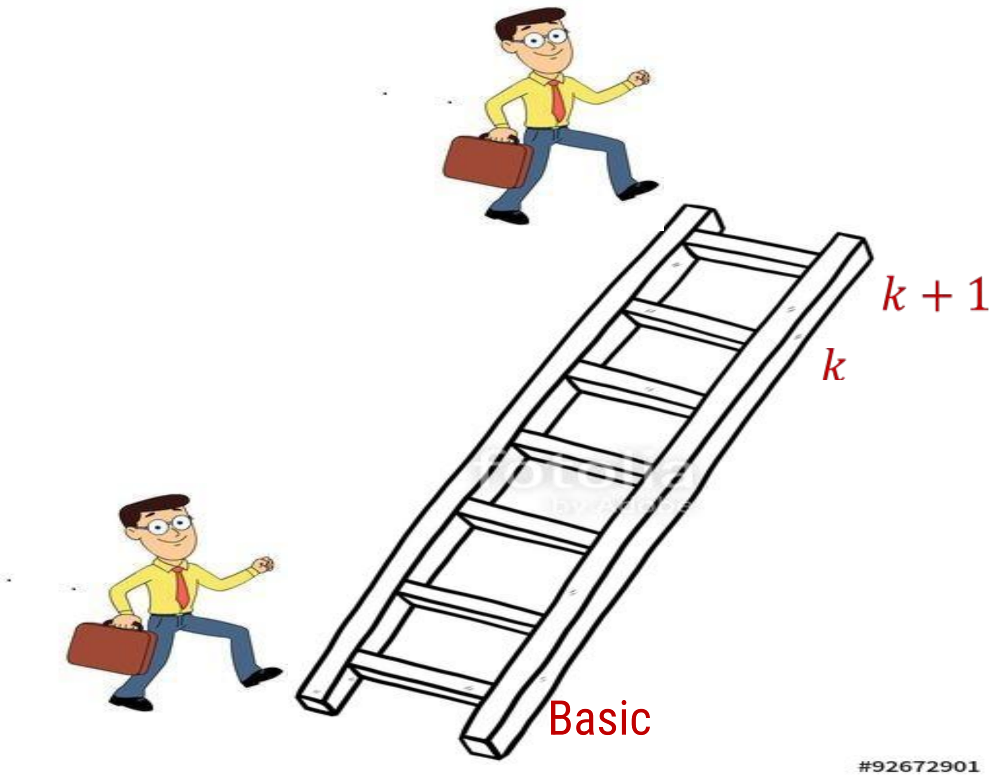
Properties of Equivalence Relations

- Assume that R is a relation on a set A, in other words, $R \subseteq A \times A$, where $(x, y) \in R$ to indicate x is related to y via Relation R.
  1. R is reflexive if for every x ∈ A, xRx
  2. R is symmetric if for every x and y in A, if xRy, then yRx
  3. R is transitive if for every x, y and z in A, if xRy and yRz, then xRz.
  4. R is an equivalence relation on A, if R is reflexive, symmetric and transitive.

Principle of Mathematical Induction

Principle of Mathematical Induction

- Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:
  1. $\mathrm{P}(\mathrm{n}_0)$ is true.
  2. For any $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.



Prove $\sum_{i=1}^{n} i = n(n+1)/2$ using PMI

Step-1: Basic step

We must show that P(1) is true.

P(1) = 1 (L.H.S)

P(1)= $1(1+1)/2$ =1, And this is obviously true.

Step-2: Induction Hypothesis

$k \geq 1$ and $1+2+3+\cdots+k = \mathbf{k(k+1)/2}$

Step-3: Proof of Induction

(by induction hypothesis)

(Hence Proved)

Prove $1 + 3 + 5 + \dots + 2n-1 = n^2$ using PMI, n>=1

Step-1: Basic step

We must show that P(1) is true.

$P(1) = 2(1)-1 = 1$ (L.H.S)

$P(1) = (1)^2 = 1$ (R.H.S)

And, this is obviously true.

Step-2: Induction Hypothesis

$k >= 1$ and

$p(k) = 1+3+5+\dots+(2k-1)=\mathbf{k^2}$

Step-3: Proof of Induction

$P(k+1) = 1+3+5+\dots+(2k-1)+(2(k+1)-1)$

$= \mathbf{k^2} + (2(k+1)-1)$

$= k^2 + (2k+2-1)$

$= k^2 + 2k+1$

$=(k+1)^2$ (Hence Proved)

Prove 7+ 13+19+…..+(6n+1)= n(3n+4) using PMI, n>=1

Step-1: Basic step

We must show that p(1) is true.

P(1)= 6n+1=(6(1)+1)=7

P(1)= n(3n+4) =1(3(1)+4)=7

And, this is obviously true.

Step-2: Induction Hypothesis

k >= 1 and

p(k) = 7+13+19+…..+(6k+1)=**k(3k+4)**

Step-3: Proof of Induction

P(k+1)= 7+13+…..+(6k+1)+(6(k+1)+1)

= **k(3k+4)**+(6(k+1)+1)

= k(3k+4)+(6k+6+1)

= $3k^2+4k+6k+7$

= $3k^2+10k+7$

= $3k^2+3k+7k+7$

= 3k(k+1)+7(k+1)

= (k+1)(3k+7)

= (k+1)(3k+3+4)

= (k+1)(3(k+1)+4) (Hence Proved)

Prove $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$ using PMI

Step-1: Basic step

We must show that p(1) is true

$P(1)=(1)^2=1$

$P(1)=\frac{1(1+1)(2(1)+1)}{6}=1$

And, this is obviously true.

Step-2: Induction Hypothesis

k >= 0 and

$P(k) = 1+4+\ldots k^2 = \frac{k(k+1)(2k+1)}{6}$

Step-3: Proof of Induction

$$
\begin{aligned}
P(k+1) &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)+6(k+1)^2}{6} \\
&= \frac{k+1}{6}[k(2k+1)+6(k+1)] \\
&= \frac{k+1}{6}[2k^2 + k + 6k + 6] \\
&= \frac{k+1}{6}[2k^2 + 7k + 6] \\
&= \frac{k+1}{6}[2k^2 + 4k + 3k + 6] \\
&= \frac{k+1}{6}[2k(k+2) + 3(k+2)] \\
&= \frac{k+1}{6}[(k+2)(2k+3)] \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2k+2+1)}{6} \\
&= (k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Prove $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ using PMI

Step-1: Basic step

We must show that p(1) is true.

$$P(1)=\frac{1}{i(i+1)} = \frac{1}{1(1+1)} = \frac{1}{2}$$

$$P(1) = \frac{1}{1+1} = \frac{1}{2}$$

And, this is obviously true.

Step-2: Induction Hypothesis

k >= 1 and

$$p(k)= \frac{1}{2} + \frac{1}{6} \ldots + \frac{1}{k(k+1)} = \frac{k}{k+1}$$

Step-3: Proof of Induction

$$p(k+1) = \frac{1}{2} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+1+1)}$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k(k+2)+1}{(k+1)(k+2)}$$

$$=(k^2+2k + 1)/(k + 1)(k + 2)$$

$$= \frac{(k+1)^2}{(k+1)(k+2)}$$

$$= \frac{(k+1)(k+1)}{(k+1)(k+2)}$$

$$= \frac{k+1}{k+2}$$

$$= \frac{k+1}{(k+1)+1}$$

Prove 1+ $\sum_{i=1}^{n} i * i! = (n+1)!$ using PMI

Step-1: Basic step

We must show that p(1) is true.

P(1)= 1+(1*1!)=1+1=2

P(1)= (1+1)! =(2)! = 2

And, this is obviously true.

Step-2: Induction Hypothesis

k >= 1 and

p(k)= 1+(1+4..+(k*k!)) = **(k+1)!**

Step-3: Proof of Induction

P(k+1)= 1+(1+4..+(k*k!) + (k+1)*(k+1)!)

= **(k+1)!** + (k+1)(k+1)!)

= (k+1)! (1+(k+1))

= (k+1)! ((k+1)+1)

= ((k+1) + 1)! (Hence Proved)

Note:
5!=5*4!
6!=6*5!
(K+1)!=(k+1)*k!

Prove that $2^n > n^3$ where $n >= 10$, Using PMI

Step-1: Basic step

We must show that p(10) is true.

$2^{10}=1024$ and $10^3=1000$

So, $1024>1000$

And, this is obviously true.

Step-2: Induction Hypothesis

For $k>=10$

$P(k)=2^k>k^3$

Step-3: Proof of Induction

$2^{k+1}>(k+1)^3$

Where, $2^{k+1}=(2^k)(2)>2^k(1.331)$

$>2^k(1.1)^3$

$>2^k(1+0.1)^3$

$>2^k(1+\frac{1}{10})^3$

$>2^k(1+\frac{1}{k})^3$ for $k>=10$

$>(\frac{k+1}{k})^3(2^k)$

$>(\frac{k+1}{k})^3(k^3)$,because $2^k>k^3$

$(2^k)(2)>(k+1)^3$

$2^{k+1}>(k+1)^3$ (Hence Proved)

Prove $n(n^2+5)$ is divisible by 6 using PMI

Step-1: Basic step

We must show that p(1) is true.

$P(1)=1(1^2+5)=1+5/6=1$

And, this is obviously true.

Step-2: Induction Hypothesis

For k>=1 and

$P(k)=k(k^2+5)$ is divisible by 6.

Step-3: Proof of Induction

$(k+1)[(k+1)^2+5]$

$= (k+1)(k^2+2k+1+5)$

$= (k+1)(k^2+2k+6)$

$=k^3+2k^2+6k+k^2+2k+6$

$=k^3+3k^2+8k+6$

$=k^3+3k^2+5k+3k+6$

$=k(k^2+5)+3k(k+1)+6$

$= k(k^2+5)+3k(k+1)+6$

- Here, $k(k^2+5)$ is divisible by 6 ,given in induction hypothesis.
- In Second term k and k+1 are consecutive. So, one number is even and one is odd. So, even number is always multiple of 2 and here 3 is also present .So, second term having (2*3) is also divisible by 6.
- Last term 6 is obviously divisible by 6.Hence proved.

Strong Principle of Mathematical Induction

- Suppose $P(n)$ is a statement involving an integer n. Then to prove that $P(n)$ is true for every $n \geq n_0$, it is sufficient to show these two things:
  1. $\mathrm{P(n_0)}$ is true.
  2. For any $k \geq n_0$, if $P(n)$ is true for every n satisfying $n_0 \leq n \leq k$, then $P(k+1)$ is true.

Prove that Integer Bigger than 2 have prime factorization using strong PMI

To prove: $P(n)$ is true for every $n \geq 2$, where $P(n)$ is the statement: n is either a prime or a product of two or more primes.

Basis step:

$P(2)$ is the statement that 2 is either prime or a product of two or more primes. This is true because 2 is a prime.

Induction Hypothesis:

$k \geq 2$, and for every n with $2 \leq n \leq k$, n is either prime or a product of two or more primes.

To prove: $k + 1$ is either prime or a product of two or more primes.

Prove that Integer Bigger than 2 have prime factorization using strong PMI

Proof of Induction

We consider two cases:

1. If $k + 1$ is prime, the statement $P(k + 1)$ is true.
2. By definition of a prime, $k + 1 = r * s$, for some positive integer r and s, neither of which is 1 or $k + 1$.

   It follows that $2 \leq r \leq k$ and $2 \leq s \leq k$. Therefore, by the induction hypothesis, both r and s are either prime or the product of two or more primes.

   Therefore, their product $k + 1$ is the product of two or more primes, and $P(k + 1)$ is true.

Languages

Language

- A set of strings all of which are chosen from some Σ^*, where Σ is a particular alphabet, is called a language. If Σ is an alphabet, and $L \subseteq \Sigma^*$, then L is said to be language over alphabet Σ.
- Language comprises of:
  - Set of characters – Σ
  - Set of strings (words) defined from set of character - Σ^*
  - Language L is defined from Σ^*, and $L \subseteq \Sigma^*$ because Σ^* contains many string which may not satisfy the rules of language.
- Example:
  - Σ = {a, b}
  - Σ^* = {^, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, …}

Operations over Language

- Operations over the language are:
  1. Concatenation
  2. Union
  3. * (Kleene closure)
  4. +

If $L_1, L_2 \subseteq \Sigma^*$ then concatenation is defined as

$$L_1L_2 = \{xy \mid x \in L_1 \; and \; y \in L_2\}$$

Example:

L_1 = {hope, fear} and L_2 = {less, fully}

hopeless

L_1L_2 = {hopeless, hopefully, fearless, fearfully}

Operations over Language

- Operations over the language are:
  1. Concatenation
  2. Union
  3. * (Kleene closure)
  4. +

If $L_1, L_2 \subseteq \Sigma^*$ then union is defined as

$$L_1 \mid L_2 = \{x \mid x \in L_1 \; or \; x \in L_2\}$$

Example:

L_1 = {hope, fear} and L_2 = {less, fully}

$L_1 \mid L_2$ = {hope, fear, less, fully}

Operations over Language

- Operations over the language are:
  1. Concatenation
  2. Union
  3. * (Kleene closure)
  4. +

If L is a set of words then by L^* we mean the set of all finite strings formed by concatenating words from S, where any word may be used as often we like, and where the null string is also included.

$$L^* = \bigcup_{i=0}^{\infty} L^i$$

Example: L = {ab}

L* = {^, ab, abab, ababab, abababab, ….}

Operations over Language

- Operations over the language are:
  1. Concatenation
  2. Union
  3. * (Kleene closure)
  4. +

If L is a set of words then by L^+ we mean the set of all finite strings formed by concatenating words from L, where any word may be used as often we like, and where the null string is not included.

$$L^+ = \bigcup_{i=1}^{\infty} L^i$$

Example: L = {ab}

L^+ = {ab, abab, ababab, abababab, ….}

Thank You